APPLIED PURPLE TEAMING

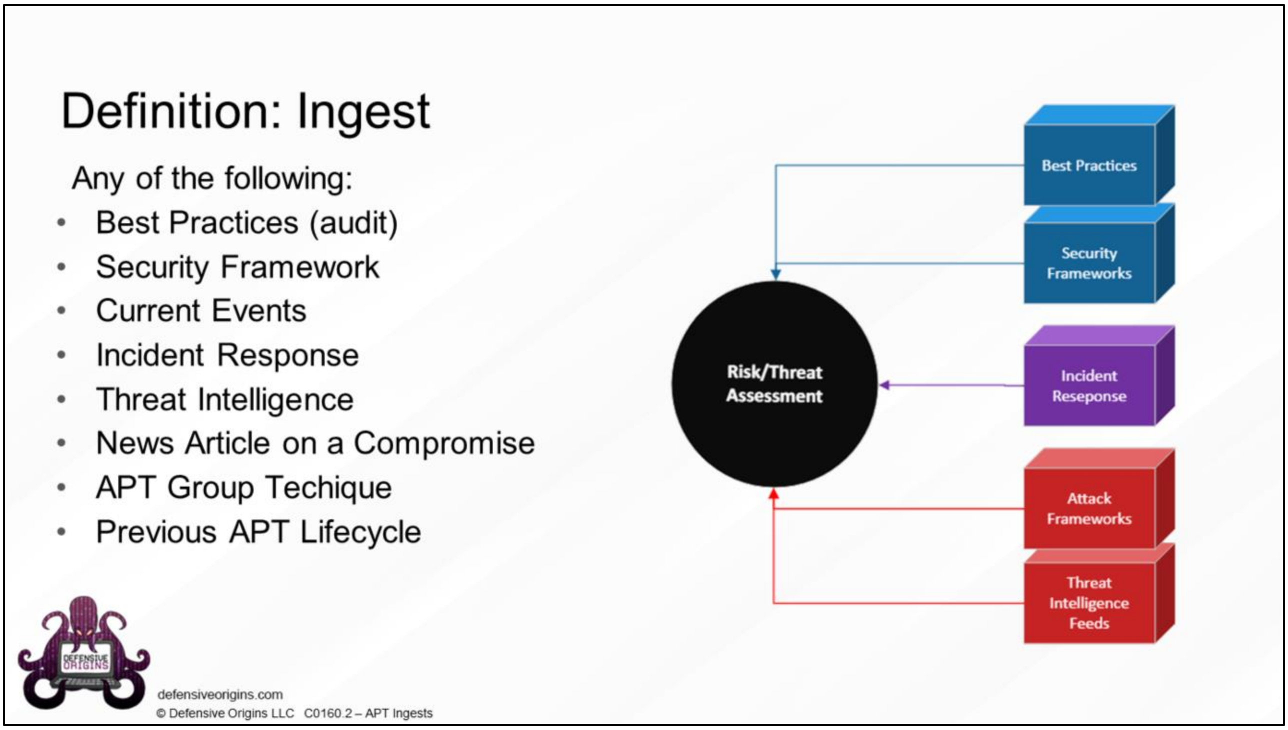
C0160

APTLC Ingests

Threat and Risk Analysis

defensiveorigins.com

Applied Purple Teaming – C0160 – Atomic Purple Team Lifecycle Ingests
Threat and Risk Analysis



Definition: Ingest

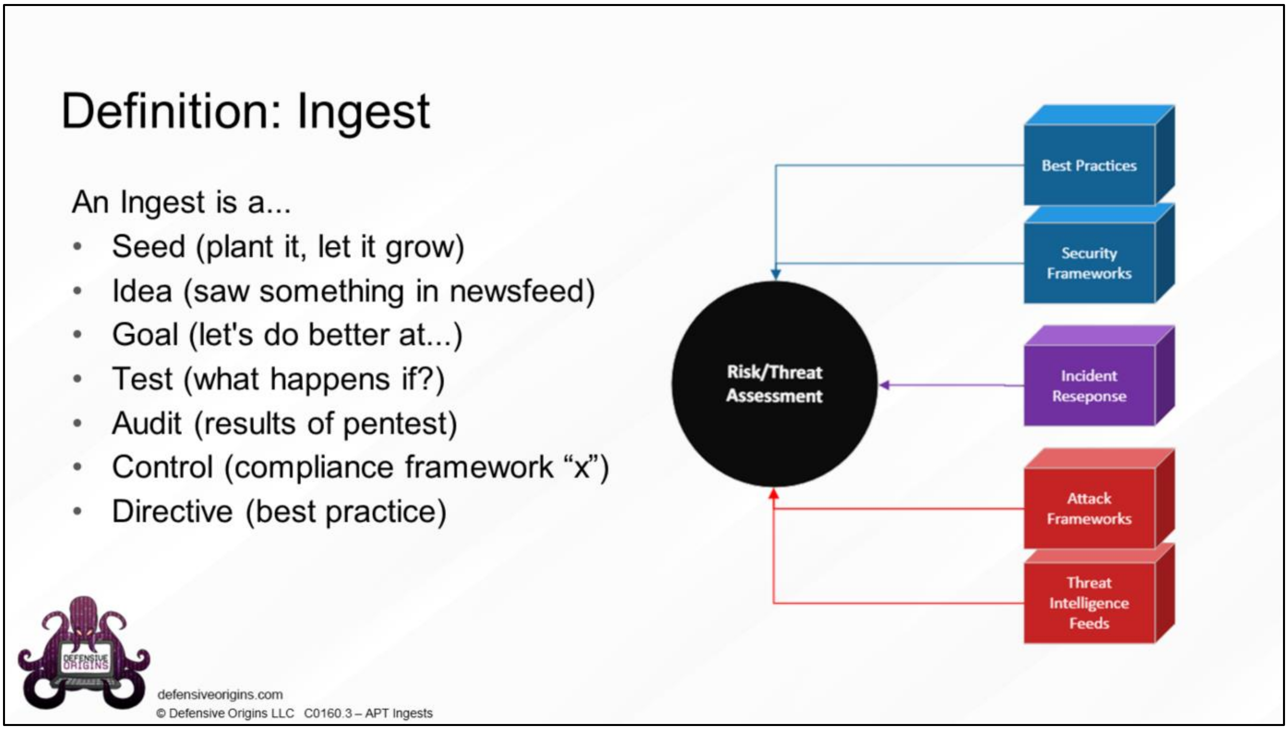
Any of the following:

- Best Practices (audit)
- Security Framework
- Current Events
- Incident Response
- Threat Intelligence
- News Article on a Compromise
- APT Group Techique
- Previous APT Lifecycle

defensiveorigins.com

C0160.2 – APT Ingests

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam



Definition: Ingest

An Ingest is a...

- Seed (plant it, let it grow)
- Idea (saw something in newsfeed)
- Goal (let's do better at...)
- Test (what happens if?)
- Audit (results of pentest)
- Control (compliance framework “x”)
- Directive (best practice)

Risk/Threat Assessment

Best Practices

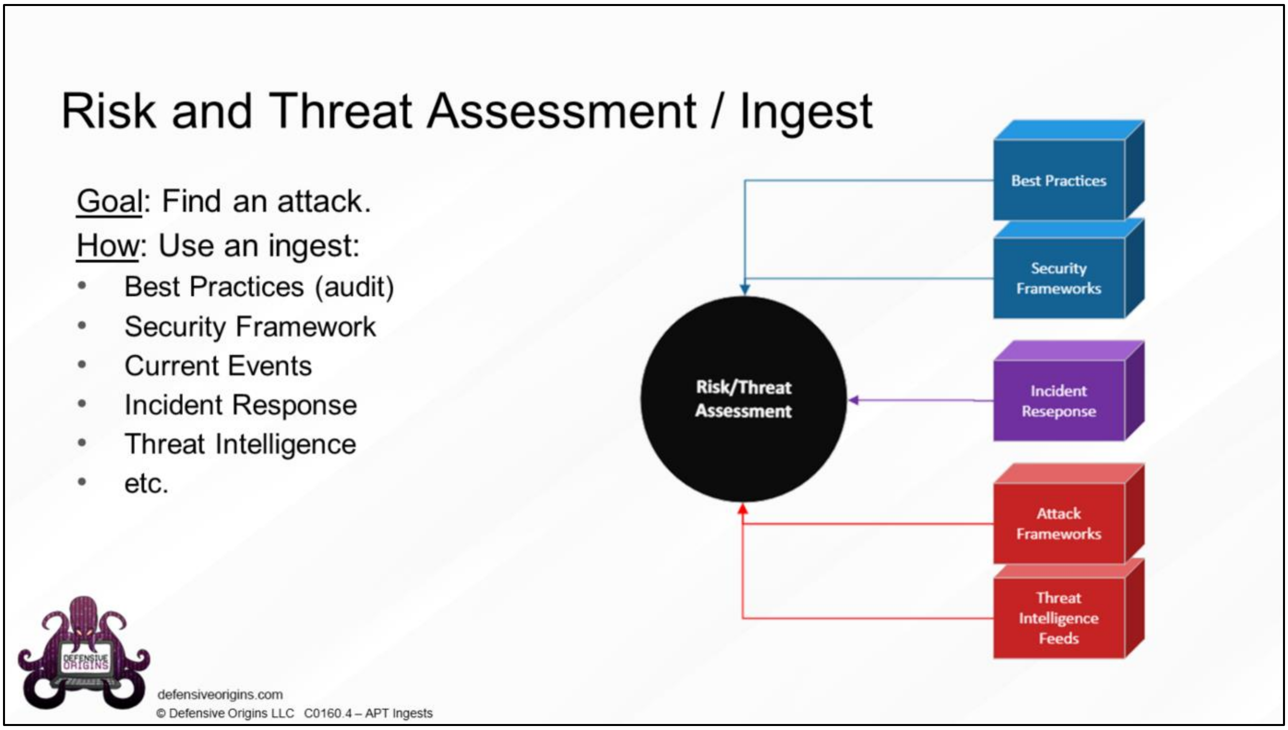
Security Frameworks

Incident Reseponse

Attack Frameworks

Threat Intelligence Feeds

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam



Risk and Threat Assessment / Ingest

Goal: Find an attack.

How: Use an ingest:

- Best Practices (audit)
- Security Framework
- Current Events
- Incident Response
- Threat Intelligence
- etc.

Risk/Threat Assessment

Best Practices

Security Frameworks

Incident Reseponse

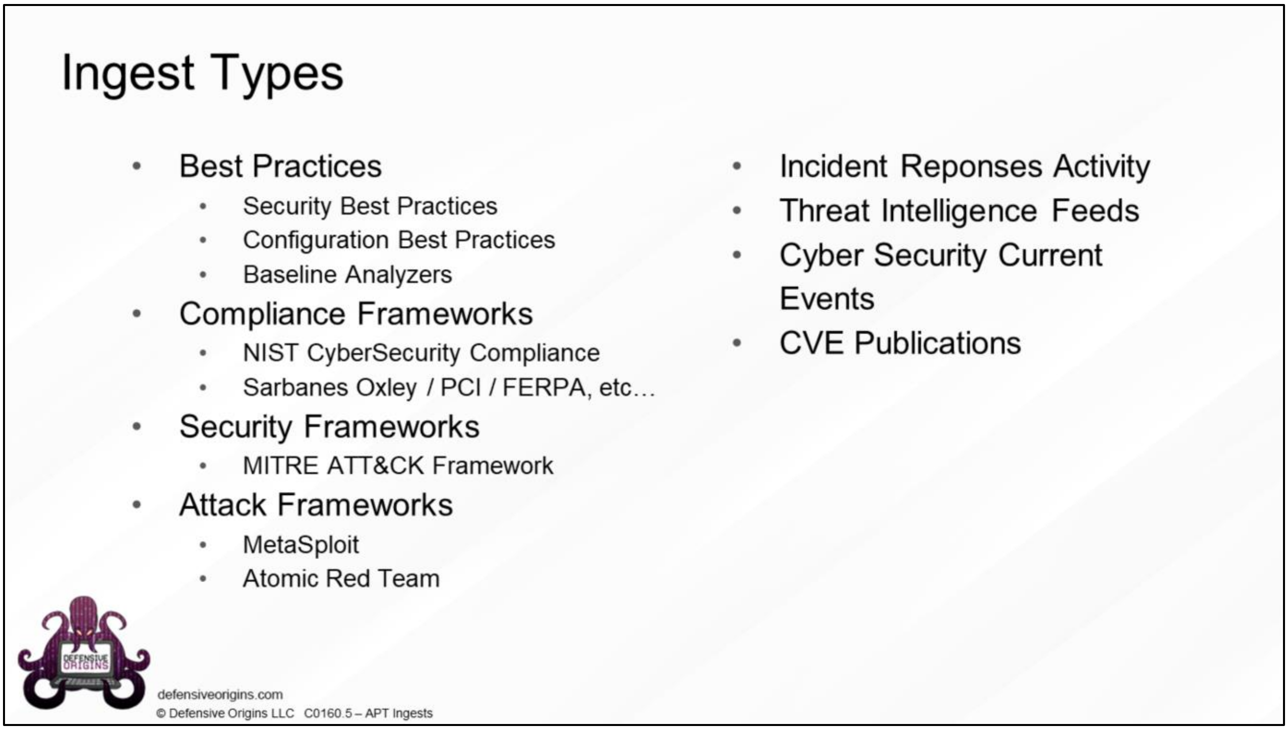
Attack Frameworks

Threat Intelligence Feeds

defensiveorigins.com

C0160.4 – APT Ingests

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam

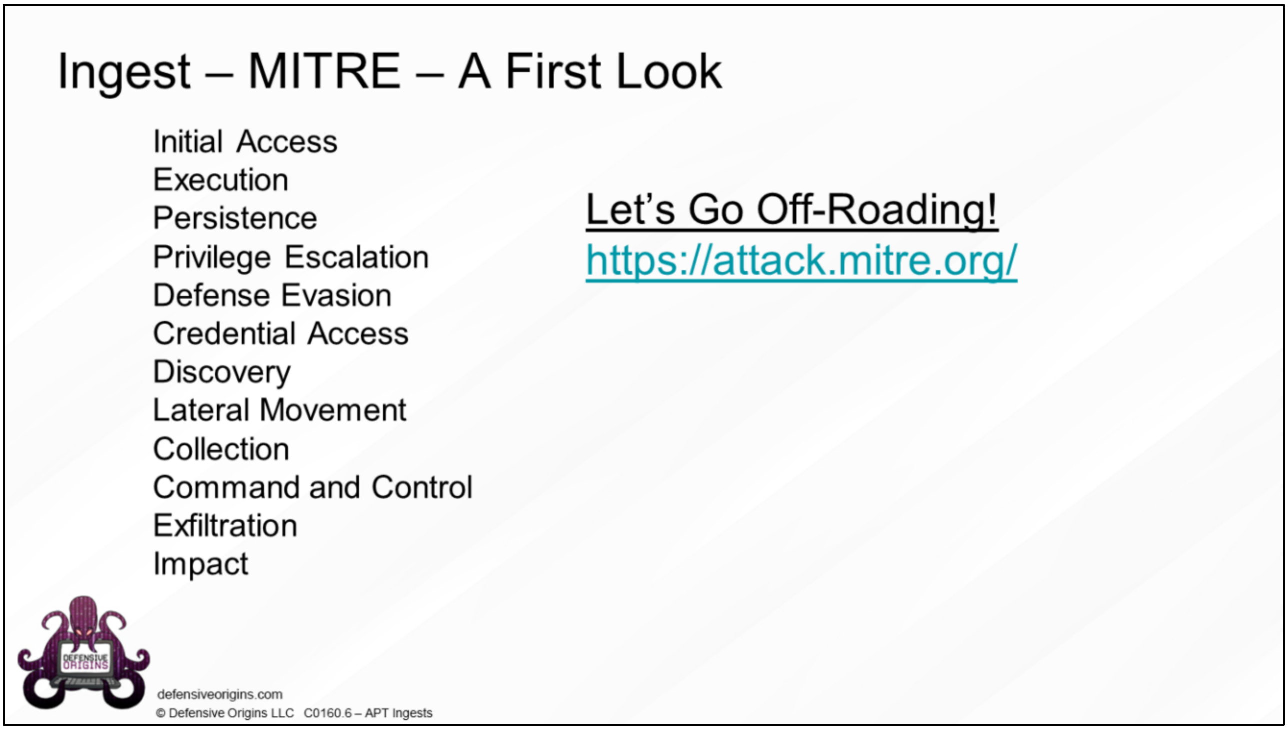


Ingest Types

- Best Practices
  - Security Best Practices
  - Configuration Best Practices
  - Baseline Analyzers
- Compliance Frameworks
  - NIST CyberSecurity Compliance
  - Sarbanes Oxley / PCI / FERPA, etc…
- Security Frameworks
  - MITRE ATT&CK Framework
- Attack Frameworks
  - MetaSploit
  - Atomic Red Team

- Incident Reponses Activity
- Threat Intelligence Feeds
- Cyber Security Current Events
- CVE Publications

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam

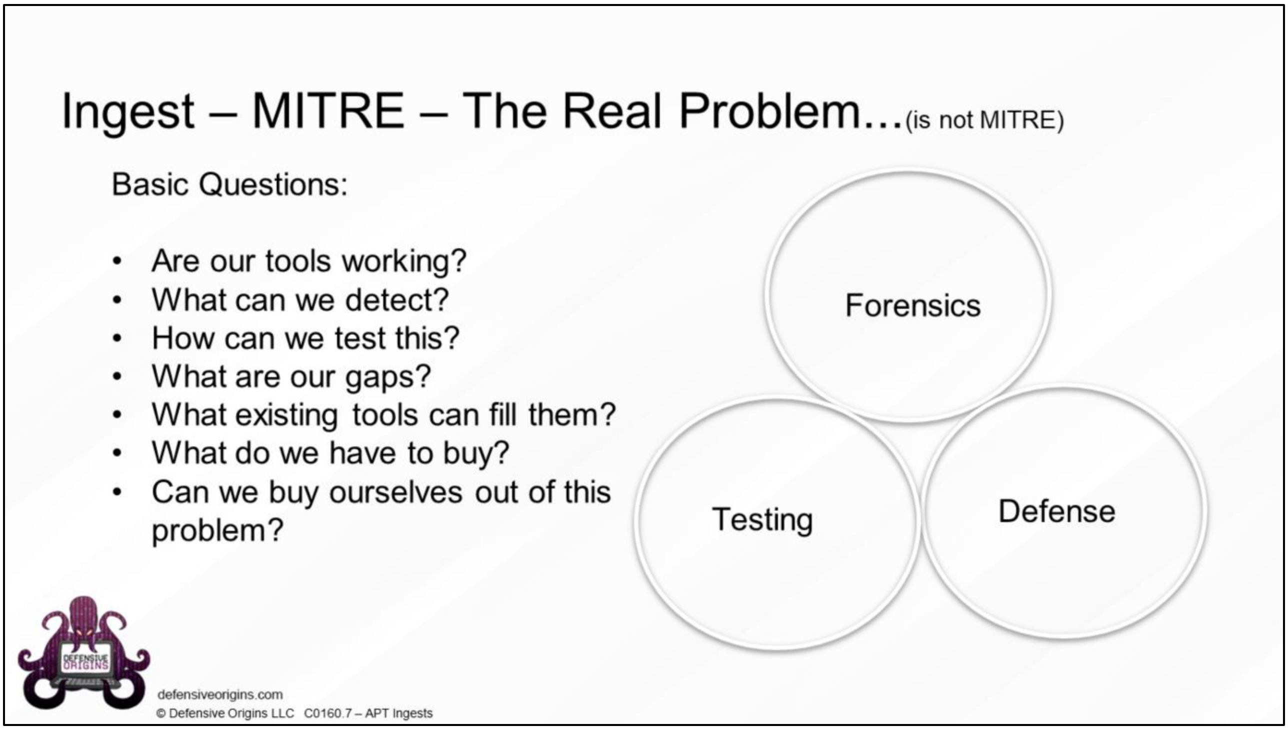


Ingest – MITRE – A First Look

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
Impact

Let’s Go Off-Roading!
https://attack.mitre.org/

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam
https://attack.mitre.org/
https://github.com/MalwareArchaeology/ATTACK



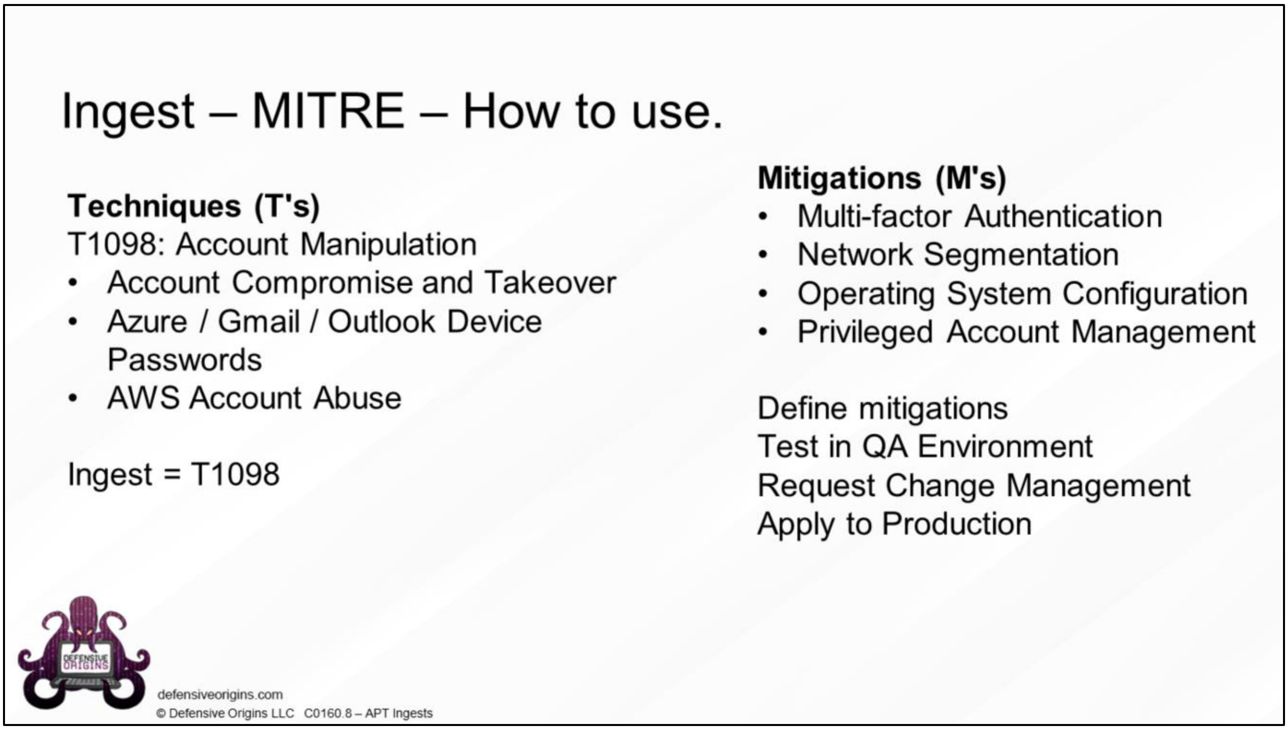
Ingest – MITRE – The Real Problem…(is not MITRE)

Basic Questions:

- Are our tools working?
- What can we detect?
- How can we test this?
- What are our gaps?
- What existing tools can fill them?
- What do we have to buy?
- Can we buy ourselves out of this problem?

Forensics
Testing
Defense

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam



Ingest – MITRE – How to use.

Techniques (T's)

T1098: Account Manipulation

- Account Compromise and Takeover
- Azure / Gmail / Outlook Device Passwords
- AWS Account Abuse

Ingest = T1098

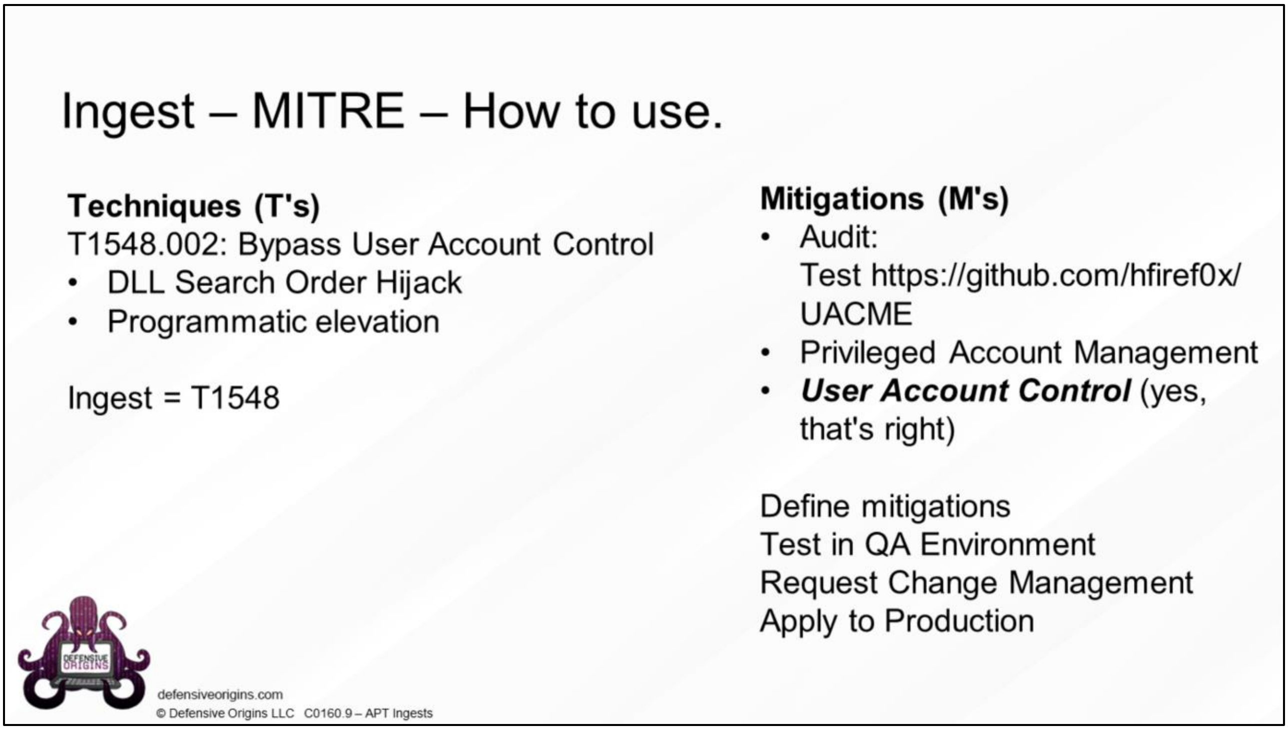
Mitigations (M's)

- Multi-factor Authentication
- Network Segmentation
- Operating System Configuration
- Privileged Account Management

Define mitigations
Test in QA Environment
Request Change Management
Apply to Production

defensiveorigins.com

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam
https://attack.mitre.org/
https://attack.mitre.org/techniques/T1098/



Ingest – MITRE – How to use.

Techniques (T's)

T1548.002: Bypass User Account Control

- DLL Search Order Hijack
- Programmatic elevation

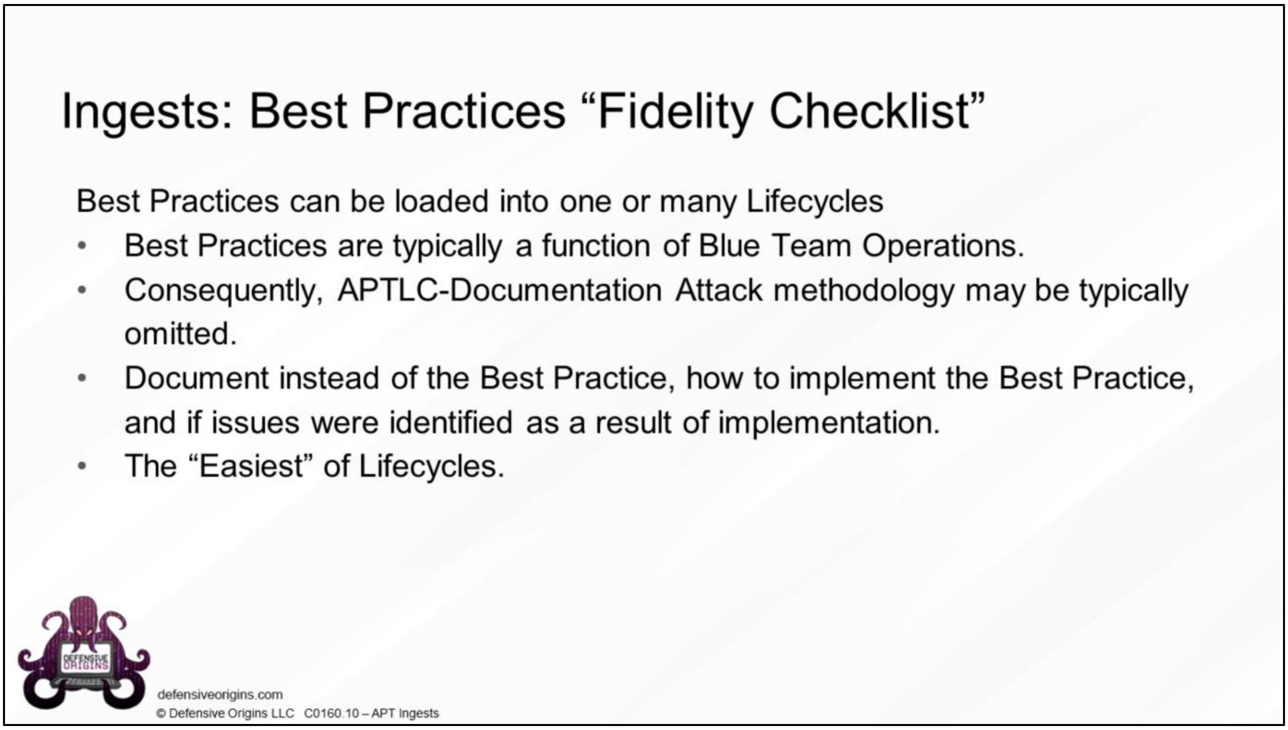
Ingest = T1548

Mitigations (M's)

- Audit:
  Test https://github.com/hfiref0x/UACME
- Privileged Account Management
- ***User Account Control*** (yes, that's right)

Define mitigations
Test in QA Environment
Request Change Management
Apply to Production

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam
https://attack.mitre.org/
https://attack.mitre.org/techniques/T1548/002/
https://github.com/hfiref0x/UACME

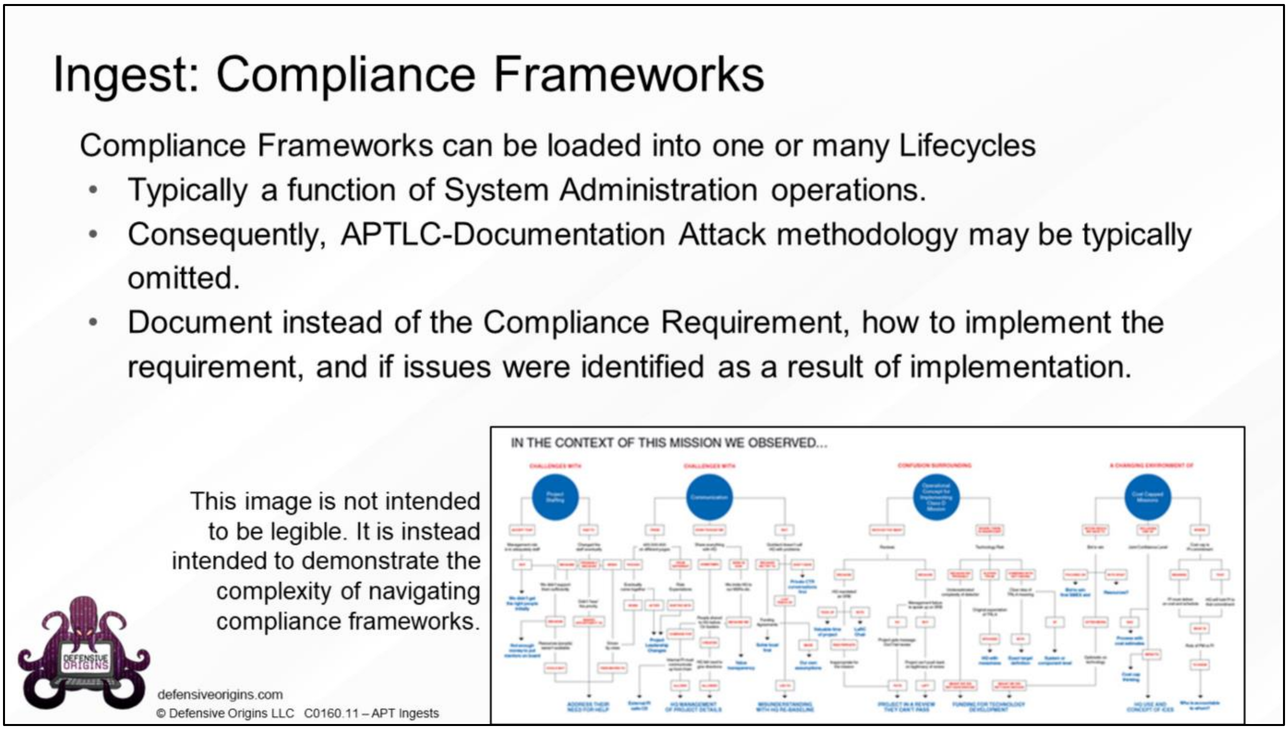


Ingests: Best Practices “Fidelity Checklist”

Best Practices can be loaded into one or many Lifecycles

- Best Practices are typically a function of Blue Team Operations.
- Consequently, APTLC-Documentation Attack methodology may be typically omitted.
- Document instead of the Best Practice, how to implement the Best Practice, and if issues were identified as a result of implementation.
- The “Easiest” of Lifecycles.

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam



Ingest: Compliance Frameworks

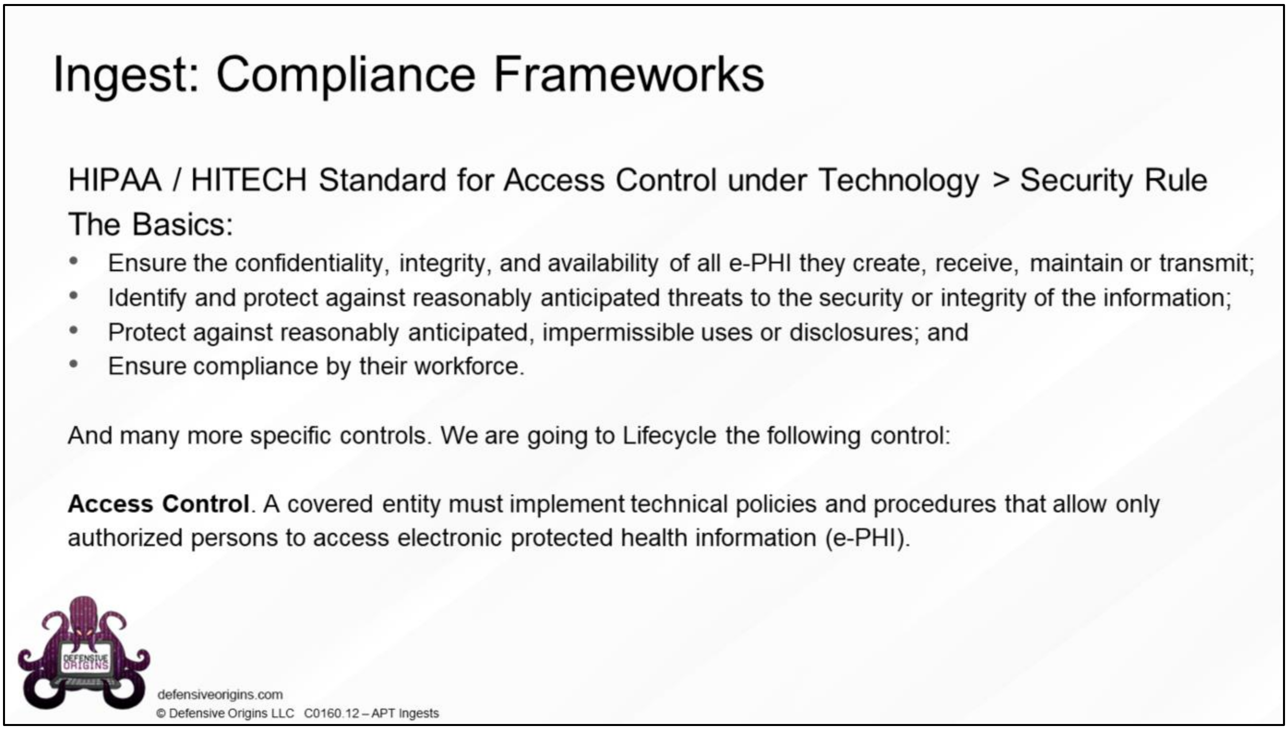
Compliance Frameworks can be loaded into one or many Lifecycles

- Typically a function of System Administration operations.
- Consequently, APTLC-Documentation Attack methodology may be typically omitted.
- Document instead of the Compliance Requirement, how to implement the requirement, and if issues were identified as a result of implementation.

This image is not intended to be legible. It is instead intended to demonstrate the complexity of navigating compliance frameworks.

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam

HIPAA: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
COBIT: https://www.isaca.org/resources/cobit
ITIL: https://www.axelos.com/best-practice-solutions/itil
SOX: https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act



Ingest: Compliance Frameworks

HIPAA / HITECH Standard for Access Control under Technology > Security Rule

The Basics:

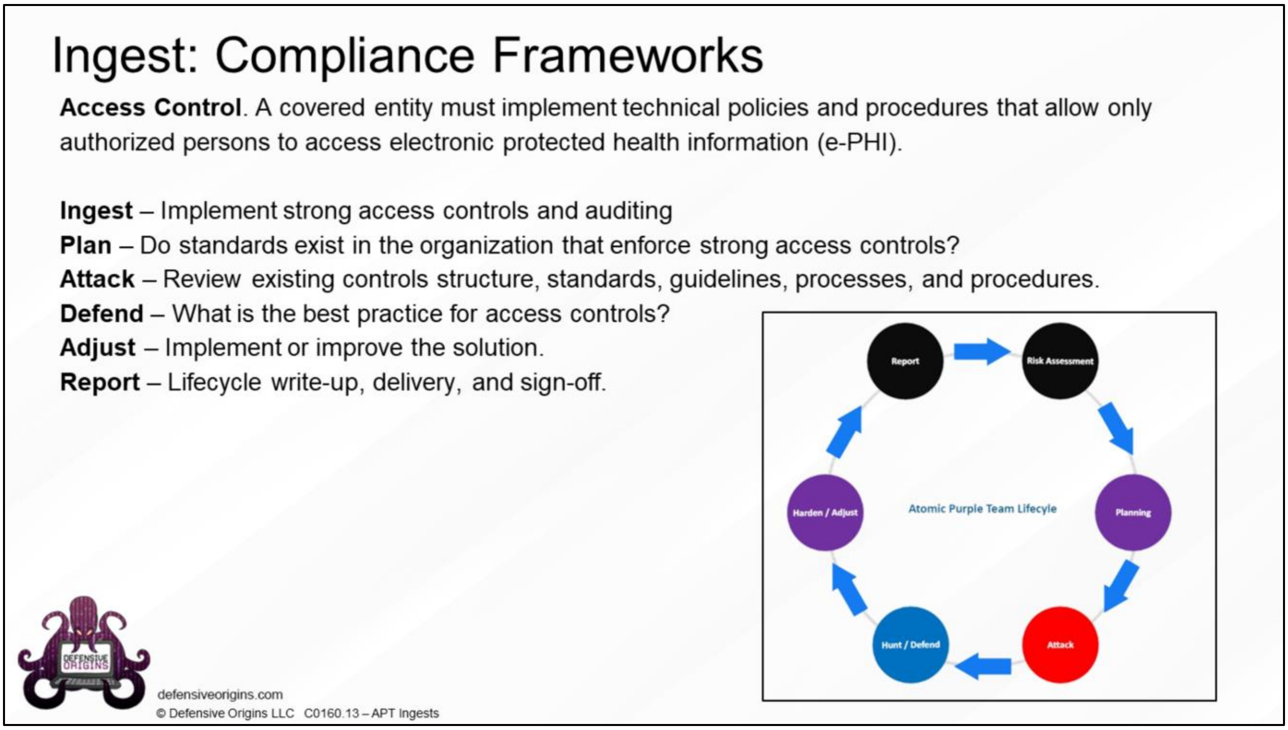
- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

And many more specific controls. We are going to Lifecycle the following control:

Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam

HIPAA: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html



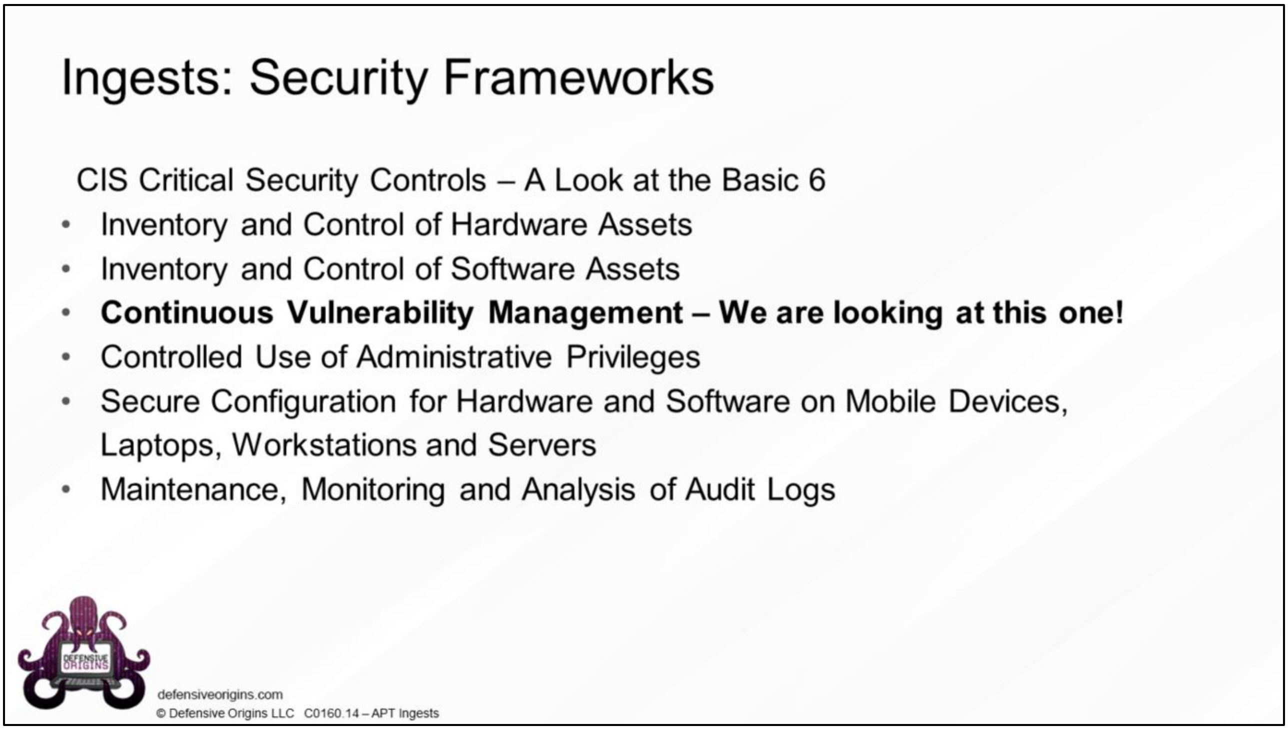
Ingest: Compliance Frameworks

Access Control. A covered entity must implement technical policies and procedures that allow only authorized persons to access electronic protected health information (e-PHI).

Ingest – Implement strong access controls and auditing
Plan – Do standards exist in the organization that enforce strong access controls?
Attack – Review existing controls structure, standards, guidelines, processes, and procedures.
Defend – What is the best practice for access controls?
Adjust – Implement or improve the solution.
Report – Lifecycle write-up, delivery, and sign-off.

defensiveorigins.com

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam



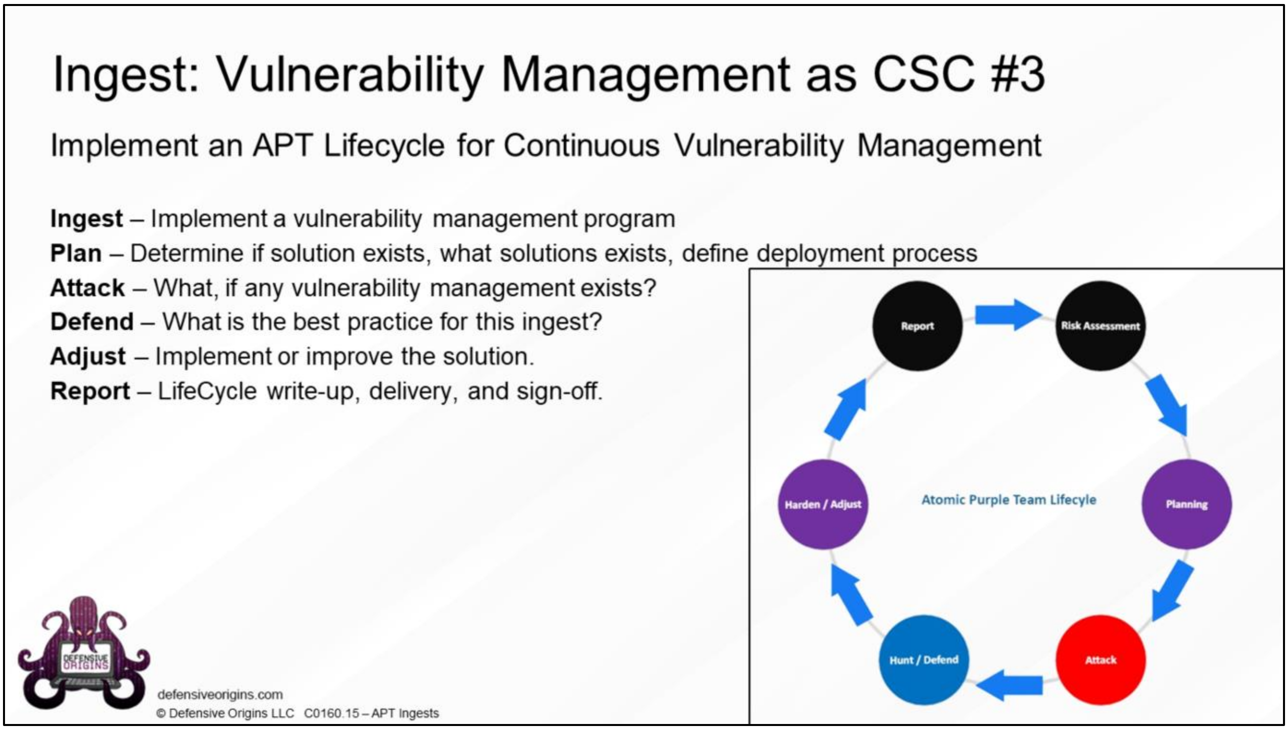
Ingests: Security Frameworks

CIS Critical Security Controls – A Look at the Basic 6

- Inventory and Control of Hardware Assets
- Inventory and Control of Software Assets
- **Continuous Vulnerability Management – We are looking at this one!**
- Controlled Use of Administrative Privileges
- Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- Maintenance, Monitoring and Analysis of Audit Logs

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam

CIS: https://www.cisecurity.org/controls/



Ingest: Vulnerability Management as CSC #3

Implement an APT Lifecycle for Continuous Vulnerability Management

Ingest – Implement a vulnerability management program
Plan – Determine if solution exists, what solutions exists, define deployment process
Attack – What, if any vulnerability management exists?
Defend – What is the best practice for this ingest?
Adjust – Implement or improve the solution.
Report – LifeCycle write-up, delivery, and sign-off.

Atomic Purple Team Lifecyle

Report

Risk Assessment

Planning

Attack

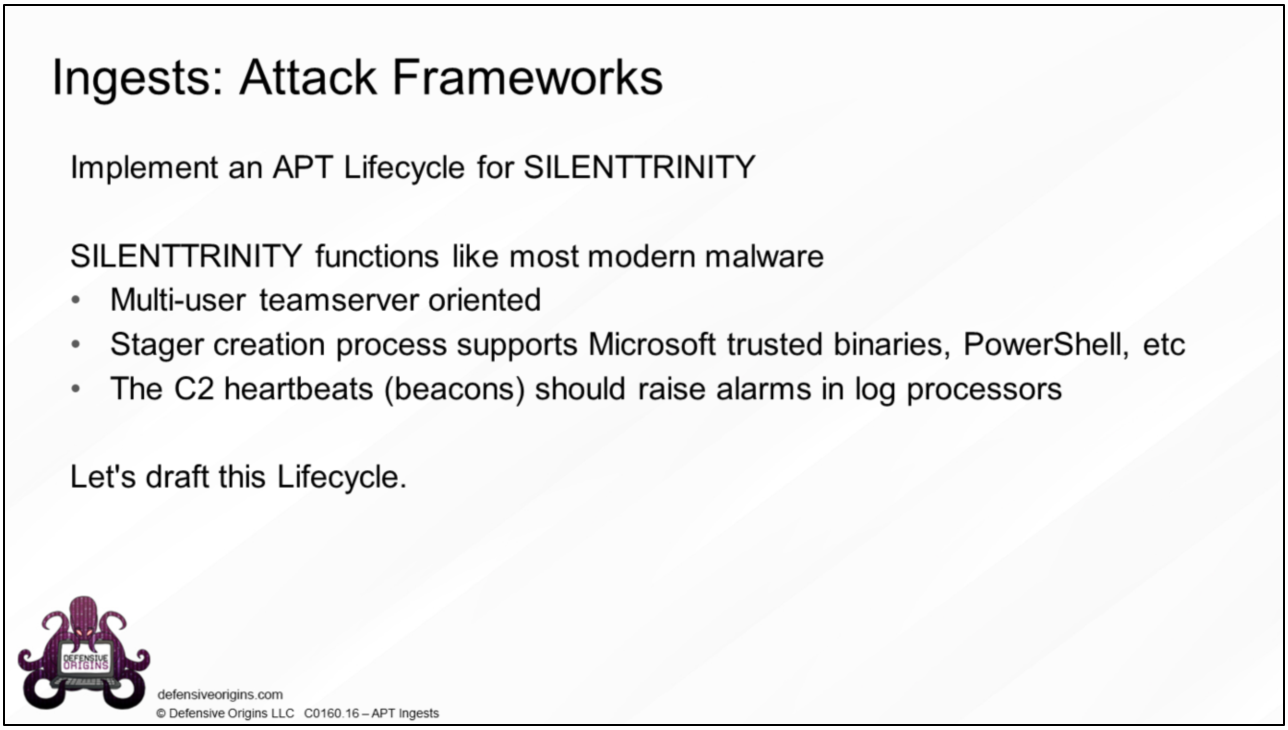
Hunt / Defend

Harden / Adjust

defensiveorigins.com
© Defensive Origins LLC C0160.15 – APT Ingests

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam

CIS: https://www.cisecurity.org/controls/



Ingests: Attack Frameworks

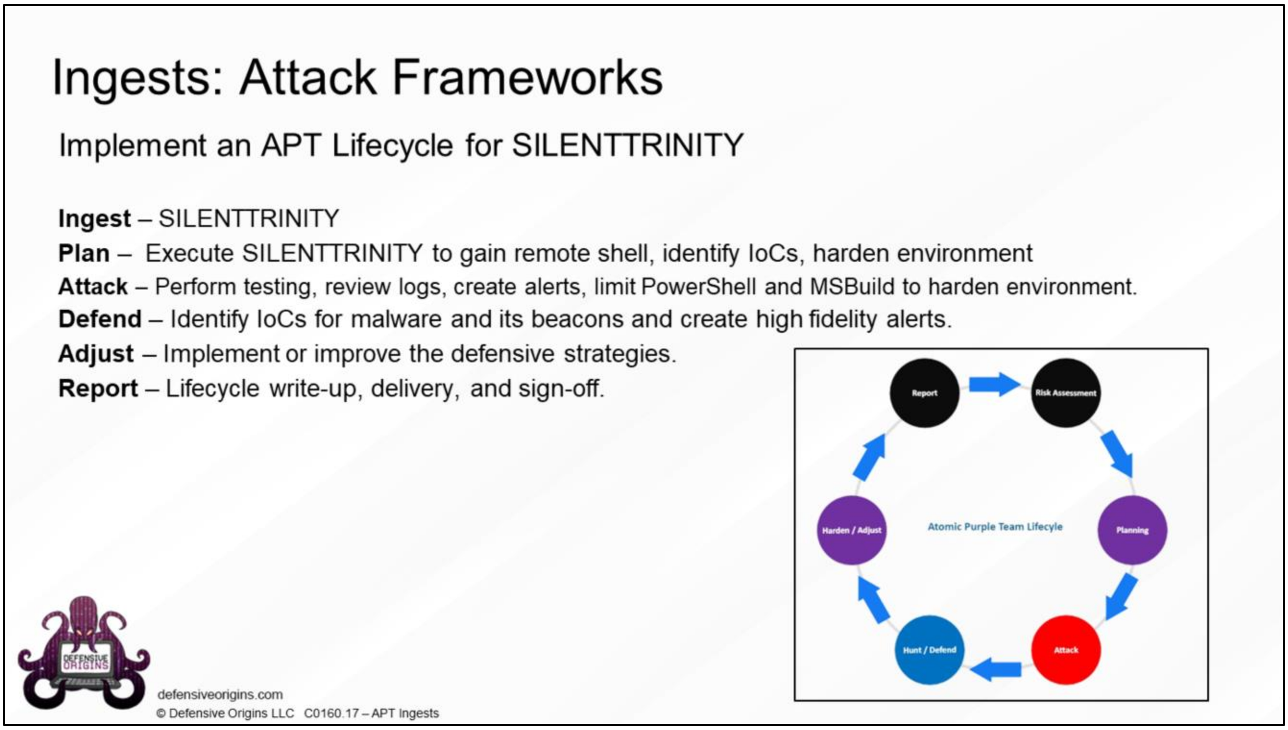
Implement an APT Lifecycle for SILENTTRINITY

SILENTTRINITY functions like most modern malware

- Multi-user teamserver oriented
- Stager creation process supports Microsoft trusted binaries, PowerShell, etc
- The C2 heartbeats (beacons) should raise alarms in log processors

Let's draft this Lifecycle.

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam
https://github.com/byt3bl33d3r/SILENTTRINITY



Ingests: Attack Frameworks

Implement an APT Lifecycle for SILENTTRINITY

Ingest – SILENTTRINITY

Plan – Execute SILENTTRINITY to gain remote shell, identify IoCs, harden environment

Attack – Perform testing, review logs, create alerts, limit PowerShell and MSBuild to harden environment.

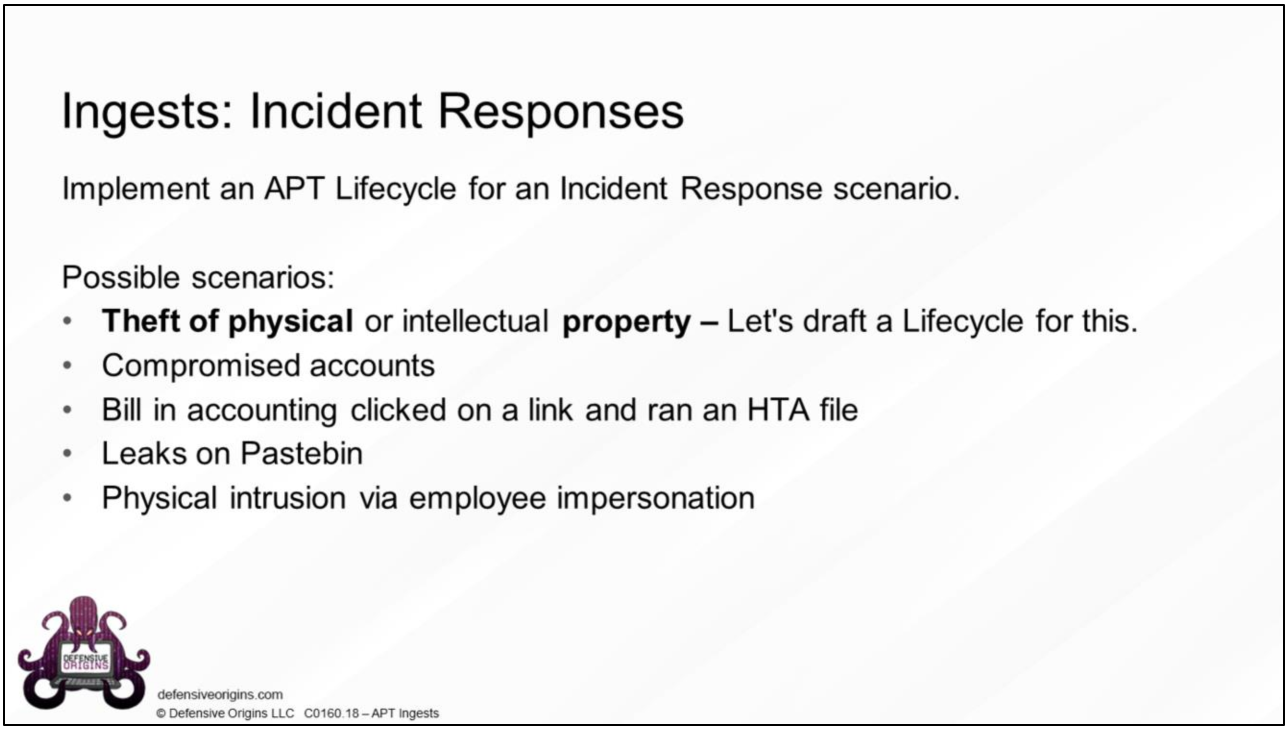
Defend – Identify IoCs for malware and its beacons and create high fidelity alerts.

Adjust – Implement or improve the defensive strategies.

Report – Lifecycle write-up, delivery, and sign-off.

defensiveorigins.com

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam
https://github.com/byt3bl33d3r/SILENTTRINITY



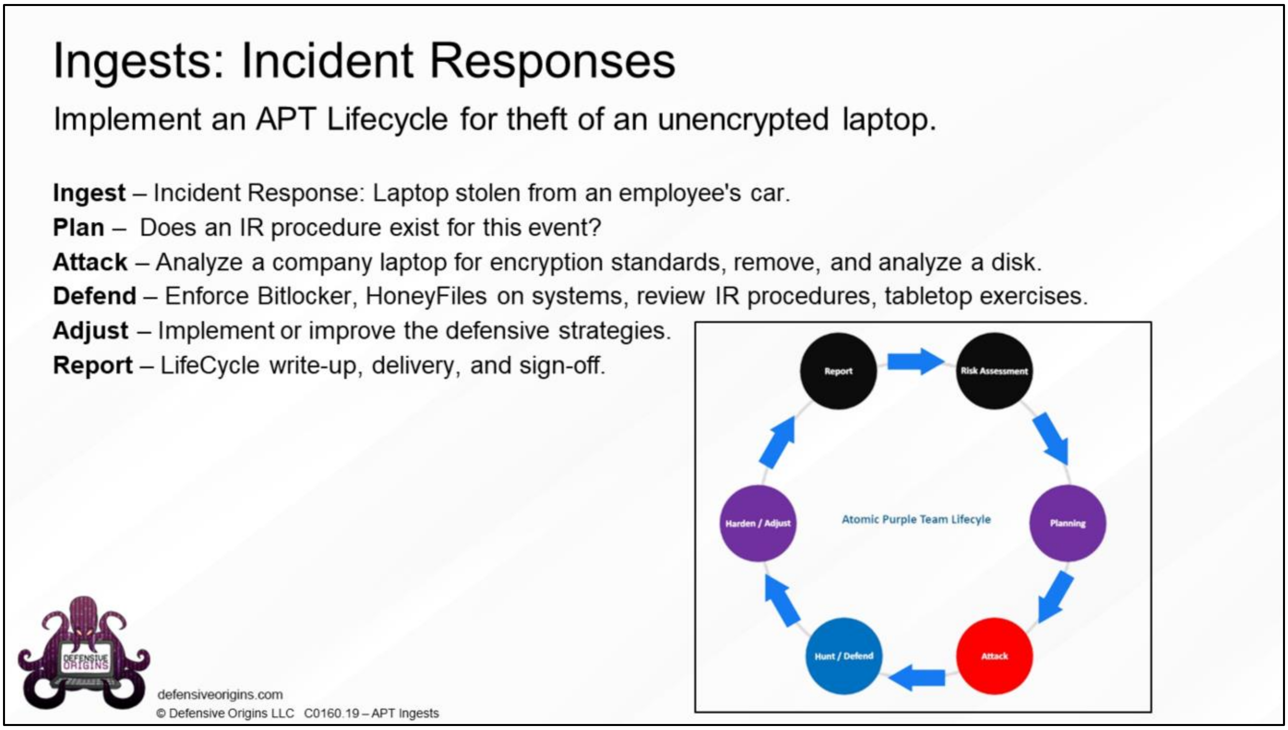
Ingests: Incident Responses

Implement an APT Lifecycle for an Incident Response scenario.

Possible scenarios:

- **Theft of physical** or intellectual **property –** Let's draft a Lifecycle for this.
- Compromised accounts
- Bill in accounting clicked on a link and ran an HTA file
- Leaks on Pastebin
- Physical intrusion via employee impersonation

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam



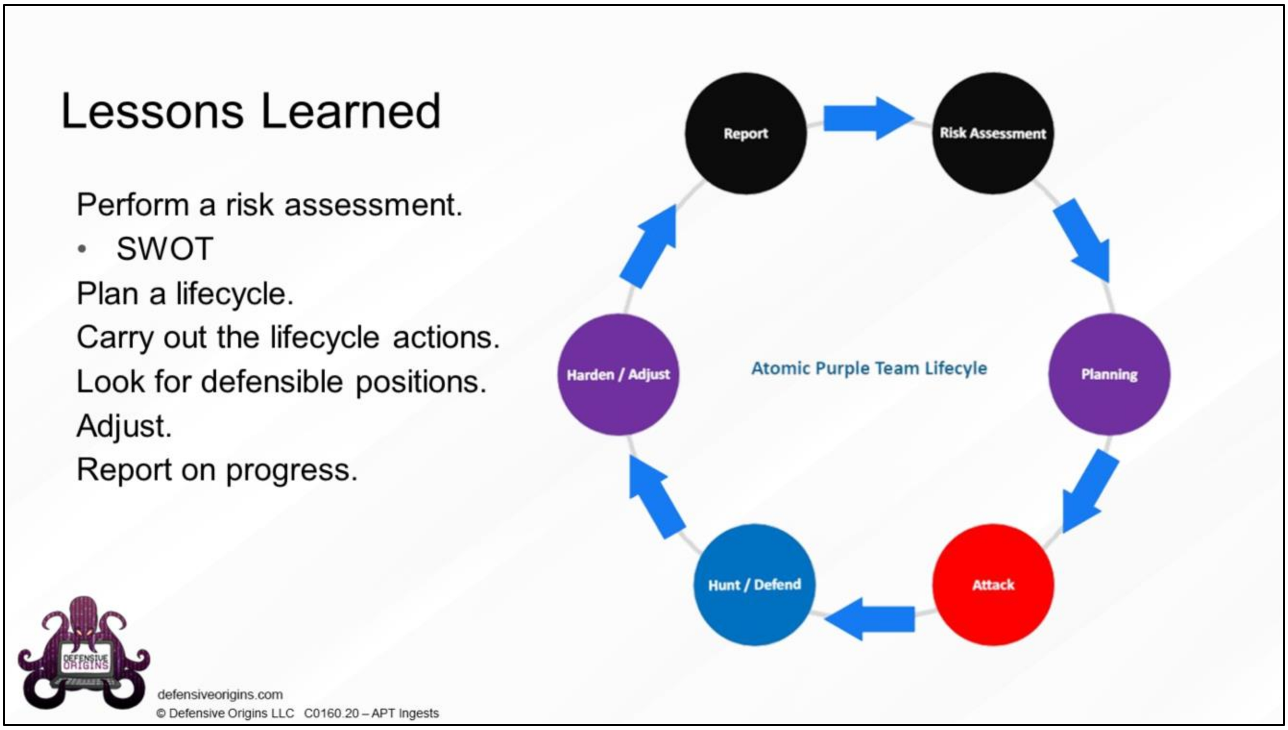
Ingests: Incident Responses

Implement an APT Lifecycle for theft of an unencrypted laptop.

Ingest – Incident Response: Laptop stolen from an employee's car.
Plan – Does an IR procedure exist for this event?
Attack – Analyze a company laptop for encryption standards, remove, and analyze a disk.
Defend – Enforce Bitlocker, HoneyFiles on systems, review IR procedures, tabletop exercises.
Adjust – Implement or improve the defensive strategies.
Report – LifeCycle write-up, delivery, and sign-off.

defensiveorigins.com
© Defensive Origins LLC C0160.19 – APT Ingests

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam



Lessons Learned

Perform a risk assessment.

- SWOT

Plan a lifecycle.

Carry out the lifecycle actions.

Look for defensible positions.

Adjust.

Report on progress.

Atomic Purple Team Lifecyle
Report
Risk Assessment
Planning
Attack
Hunt / Defend
Harden / Adjust

defensiveorigins.com

Links:
https://github.com/DefensiveOrigins/AtomicPurpleTeam